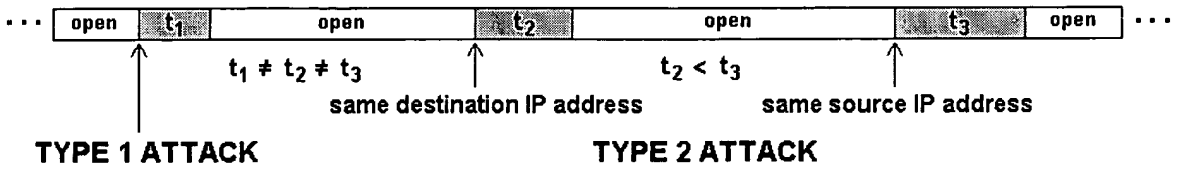
specific aspects of the claimed invention, which so far have not been shown to exist in the prior art before the effective date (August 18, 1999) of the present application.

1. The cited prior art does not teach preventing certain IP packets from entering a network only for a predetermined time, the duration of which is predetermined corresponding to the detected type of attack, and then reopening the gateway to allow such IP packets to enter the network.

As has been argued in previous responses, according to the claimed invention, when an attack is detected from among the stored IP packets, only then the IP packets associated with the detected attack are prevented from entering the network, and only then for a predetermined period of time. Moreover, the predetermined time depends, in a flexible manner, on the type of attack. Thus, unlike traditional firewall protection, IP packets associated with an attack are not shut off completely, but rather the ingress of such IP packets is prevented only "for a predetermined time" sufficient to stop the attack, and thereafter, the gateway is reopened. (See, page 14, line 11, to page 15, line 20, of applicant's response to the final Office Action.)

2. The cited prior art does not teach a flexible system, wherein the duration for which IP packets are prevented from entering the network varies depending on the type of attack detected.

Another feature of the present invention, an example of which is set forth in claim 18, is that the duration (i.e., the claimed "predetermined time") for which the gateway is closed to traffic is not a fixed time period, but rather varies adaptively, depending on the type of attack detected and the processing applied to the attack. An example represented by the features recited in claim 18 is illustrated in the figure below.




This diagram illustrates, in the respective shaded portions, three different predetermined times $t_1$, $t_2$, $t_3$ during which the gateway is closed, as a result of corresponding predetermined processes that are applied to attacks of the first type (TYPE 1 ATTACK) and the second type (TYPE 2 ATTACK). Because the processes applied to the detected attacks are different, the predetermined times $t_1$, $t_2$, $t_3$ when the gateway is closed are not necessarily equal to each other. As shown above, when a TYPE 1 attack is detected, a process is implemented so that the gateway is closed for a predetermined period $t_1$ and then the gateway is reopened. When a TYPE 2 attack is detected, there are two possibilities, one in which incoming IP packets have the same destination IP address as the stored Syn IP packets, and one in which the incoming IP packets have the same source IP address as the stored Syn IP packets. When the IP packets have the same destination IP address as the stored Syn IP packets, the gateway is closed for a predetermined period $t_2$, which need not equal the time $t_1$. Further, as set forth in claim 18, during a TYPE 2 attack, when the incoming IP packets have the same source IP address as the stored Syn IP packets, the gateway is closed for a different predetermined time $t_3$, which is longer than the predetermined time $t_2$ ($t_2 < t_3$).

Accordingly, this important feature of the claimed invention relates to the conditions under which the gateway is closed to Internet traffic (IP packets), including processes performed to detect cracker attacks and the resultant *durations* for which the gateway is closed in response to detected attacks. The durations differ depending on the type of attack detected and the processing undertaken to counter the attack.

Similar limitations, also setting forth and claiming a variable duration for respective "predetermined time periods," depending on the type of attacks detected and the predetermined processes applied thereto, appear in other claims, especially claims 18, 21 and 24. Of course, the Examiner is requested to give careful and independent consideration to the features set forth in each of the dependent claims.

The aim of the present invention is to keep the gateway open to IP packets to the greatest extent possible, while minimizing the time that the gateway is closed. While the prior art cited thus far has demonstrated firewall methods for closing a gateway and continuously blocking IP packets, based on detection of different types of cracker attacks that exploit deficiencies in the Internet Protocol (IP), the cited prior art does not discuss or implement different remedial processes, which determine satisfactory conditions, including variable time periods, for *reopening* the gateway to blocked IP packets.

Respectfully submitted,

Paul A. Guss
Reg. No. 33,099
Attorney for Applicant

CS-02-000131

775 S. 23rd St. #2
Arlington, VA 22202
Tel. 703-486-2710